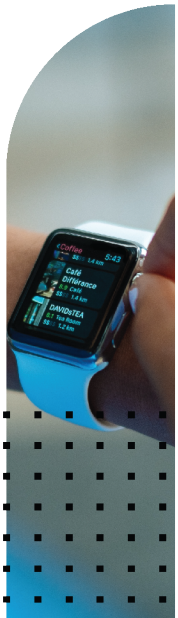
Release Notes

FortiSwitchOS 7.0.5



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 14, 2022
FortiSwitchOS 7.0.5 Release Notes
11-705-819463-20221214

TABLE OF CONTENTS

Change log

Date	Change Description
July 25, 2022	Initial release for FortiSwitchOS 7.0.5
July 28, 2022	Added a new feature.
October 10, 2022	Updated the “Product integration and support” section.
November 15, 2022	Added bug 837168 as a known issue.
November 16, 2022	Updated the description of bug 837168.
November 30, 2022	Added bug 861492 as a known issue.
December 7, 2022	Added bug 833450 as a known issue.
December 8, 2022	Updated the description of bug 833450.
December 14, 2022	Added bug 866231 as a known issue.

Introduction

This document provides the following information for FortiSwitchOS 7.0.5 build 0086.

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.0.5 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424D, FS-424D-FPOE, FS-424D-POE, FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448D, FS-448D-FPOE, FS-448D-POE, FS-448E, FS-448E-POE, FS-448E-FPOE
FortiSwitch 5xx	FS-524D-FPOE, FS-524D, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1024E, FS-1048D, FS-1048E, FS-T1024E
FortiSwitch 3xxx	FS-3032D, FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in FortiSwitchOS 7.0.5

Release 7.0.5 provides the following new features:

- A new command allows you to enable or disable bridge protocol data unit (BPDU) learning:

```
config switch global
   bpdu-learn {enable | disable}
end
```

  By default, BPDU learning is enabled. This command is available on the following FortiSwitch models:
  - FSR-124D
  - FS-224D-FPOE
  - FS-224E
  - FS-224E-POE
  - FS-248D
  - FS-248E-POE
  - FS-248E-FPOE
  - FS-424D
  - FS-424D-POE
  - FS-424D-FPOE
  - FS-424E
  - FS-424E-POE
  - FS-424E-FPOE
  - FS-424E-Fiber
  - FS-M426E-FPOE
  - FS-448D
  - FS-448D-POE
  - FS-448D-FPOE
  - FS-448E
  - FS-448E-POE
  - FS-448E-FPOE
  - FS-524D
  - FS-524D-FPOE
  - FS-548D
  - FS-548D-FPOE
  - FS-1024D
  - FS-1024E
  - FS-T1024E
  - FS-1048D
  - FS-1048E
  - FS-3032D
  - FS-3032E

Refer to the FortiSwitch feature matrix for details about the features supported by each FortiSwitch model.

Special notices

Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 to versions earlier than FortiSwitchOS 6.2.6 or 6.4.4 is not supported.

Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first

Because FortiSwitchOS 7.0.0 changed from SHA1 to SHA256 encryption for admin passwords, you need to convert the format of the admin password before downgrading from FortiSwitchOS 7.0.0 and later to an earlier FortiSwitchOS version.

If you do not convert the admin password before downgrading from FortiSwitchOS 7.0.0 and later, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

The encrypted admin password in FortiSwitchOS 7.0.0 and higher starts with “SH2”, and the encrypted admin password for earlier FortiSwitchOS versions starts with “AK1”.

To convert the format of the admin password in FortiSwitchOS 7.0.0 and later before downgrading to an earlier FortiSwitchOS version:

1. Enter the following CLI command to convert the admin password from SHA256 to SHA1 encryption:

   ```
   execute system admin account-convert <admin_name>
   ```

2. Downgrade your firmware.

Connecting multiple FSR-112D-POE switches

The FSR-112D-POE switch does not support interconnectivity to other FSR-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitchOS 7.0.5 supports upgrading from FortiSwitchOS 3.5.0 and later.

For FortiSwitch units managed by FortiGate units, refer to the FortiSwitch Devices Managed by FortiOS Release Notes for upgrade information.

Product integration and support

FortiSwitchOS 7.0.5 support

The following table lists FortiSwitchOS 7.0.5 product integration and support information.

Web browser	• Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	Refer to the FortiLink Compatibility table to find which FortiSwitchOS versions support which FortiOS versions.

Resolved issues

The following issues have been fixed in FortiSwitchOS 7.0.5. For inquiries about a particular bug, please contact Customer Service & Support.

784987	SNMP index numbers should be assigned the same for split ports and regular ports.
787797	The FortiSwitch unit does not allow VTP traffic between Cisco switches.
796030	The SNMP agent should be able to poll loopback interfaces.
796655	The *Switch* > *Monitor* > *802.1x Status* page does not sort the MAC addresses correctly and does not display VLAN traffic.
796779	The *Switch* > *Monitor* > *IGMP Snooping* page does not display IGMP groups.
796806	The `set cfg-save revert` command under `config system global` now reboots the FortiSwitch unit after waiting the number of seconds configured in the `set cfg-revert-timeout` command.
802529	After rebooting a FortiSwitch unit, IP source guard with DHCP snooping does not work.
802634	Using the `set poe-alarm-threshold` command does not work.
802786	Virtual IP addresses cannot be used in a FortiGate device to redirect the public IP address to the private IP address of the FortiSwitch unit.
803579	The “port24 Overload state. POE disabled” message appears in the log every hour.
807291	After updating the FortiSwitchOS 7.2.0, the switch fails with an “Out of memory: kill process” log message.
814741	MAC authentication bypass (MAB) authentication sometimes does not work on a managed FS-108E.
816749	After enabling `flood-unknown-multicast`, the IGMP-snooping querier port does not work.
818959	The DHCP server does not allow DHCP clients to move from one interface to another.
824605	The object identifier (OID) 1.3.6.1.2.1.10.7.2.1.19 does not work on FS-1048E.
824283	The output of the `diagnose switch physical-ports qos-stat list` command shows the same number of dropped packets for queue 0 for all ports.
825614	The status of the second power supply unit is incorrectly reported as “Not OK.”

Common vulnerabilities and exposures

FortiSwitchOS 7.0.5 is no longer vulnerable to the following vulnerabilities and exposures:

- CWE-200
- CWE-329

- CWE-352
- CWE-610

Visit https://fortiguard.com/psirt for more information.

Known issues

The following known issues have been identified with FortiSwitchOS 7.0.5. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANs).
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
463161	Upgrading the FS-448D from FortiSwitchOS 3.5.6 to 3.6.3 fails with an “Invalid root configuration data.” error.
480605	When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server. **Workarounds:** —Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN. —Temporarily disable dhcp-snooping on vlan, issue the `execute interface dhcpclient-renew <interface>` command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
510943	The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values. **Workaround:** When using the cable diagnostics feature on a port (with the `diagnose switch physical-ports cable-diag <physical port name>` CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.
542031	For the 5xx switches, the `diagnose switch physical-ports led-flash` command flashes only the SFP port LEDs, instead of all the port LEDs.
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.
572052	Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters. **Workaround:** Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.
585550	When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.

Bug ID	Description
606044/610149	The results are inaccurate when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
609375	The FortiSwitchOS supports four priority levels (critical, high, medium, and low); however, The SNMP Power Ethernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB.
667079	For the FSR-112D-POE model: • If you have enabled IGMP snooping or MLD snooping, the FortiSwitch unit does not support IPv6 functionalities and cannot pass IPv6 protocol packets transparently. • If you want to use IGMP snooping or MLD snooping with IPv6 functionalities, you need to enable `set flood-unknown-multicast` under the `config switch global` command.
673433	Some 7-meter DAC cables cause traffic loss for the FS- 448E model.
724813	The `set enforce-first-as {disable | enable}` command should have been placed under `config neighbor` and does not work in its current location (directly under `config router bgp`). There is no patch available for this issue.
784585	When a dynamic LACP trunk has formed between switches in an MRP ring, the MRP ring cannot be closed. Deleting the dynamic LACP trunk does not fix this issue. MRP supports only physical ports and static trunks; MRP does not support dynamic LACP trunks. **Workaround:** Disable MRP and then re-enable MRP.
833450	Do not use multicast IP addresses in the ranges of 224-239.0.0.x and 224-239.128.0.x on the FS-2xxD, FS-2xxE, FS-4xxD, and FS-4xxE models.
837168	The following switches make a high fan noise: • FS-224D-FPOE • FS-224E-POE • FS-248D • FS-424D • FS-424D-POE • FS-424D-FPOE • FS-448D • FS-448D-FPOE
861492	The mgmt interface MAC address is set to 00:01:02:03:04:05 after a reboot or factory reset.
866231	The `set status down` command (under `config switch physical-port`) does not work on the SFP+ ports on the FS-426E-FPOE for certain versions of FortiSwitchOS. If you need to shut down any of the SFP+ ports on the FS-426E-FPOE, do not use FortiSwitchOS 7.0.5, 7.2.0, 7.2.1, or 7.2.2. **Workaround:** Upgrade to FortiSwitchOS 7.2.3.

www.fortinet.com